

FIG. 1

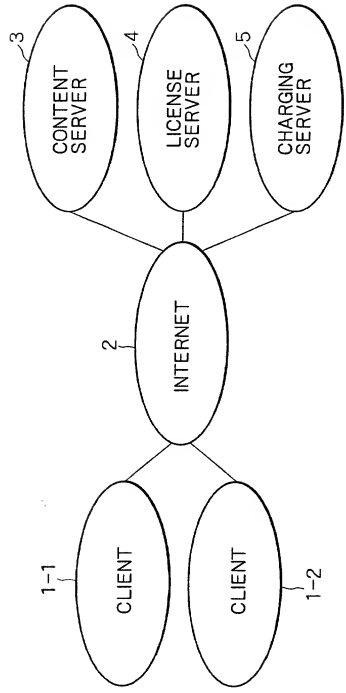


FIG. 2

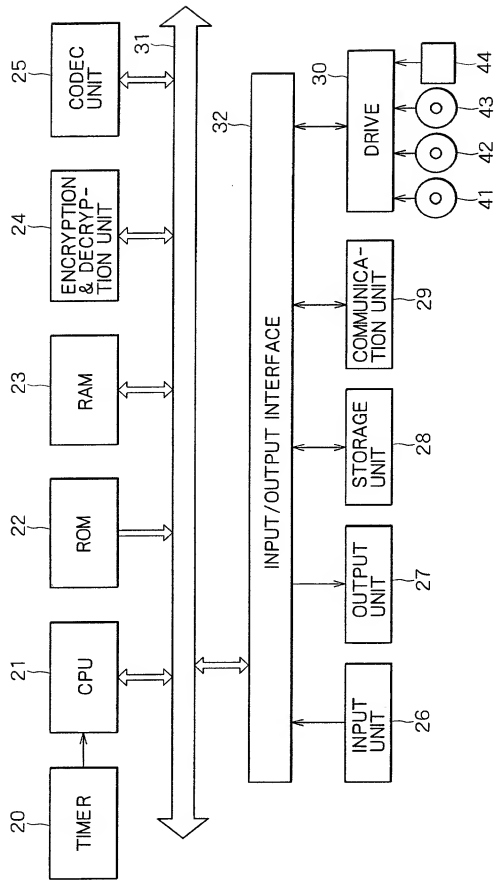


FIG. 3

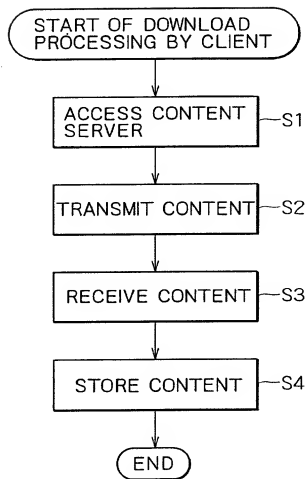
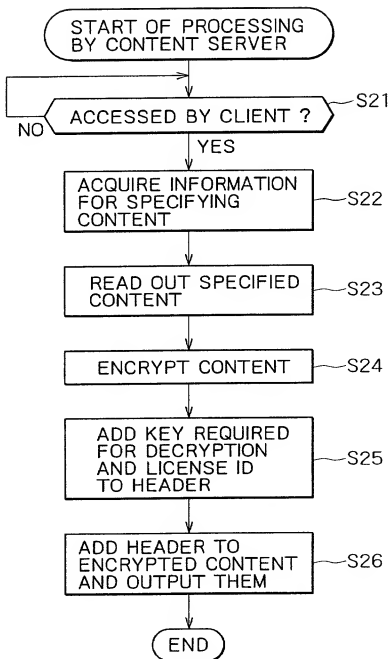


FIG. 4



10072409-120802

FIG. 5

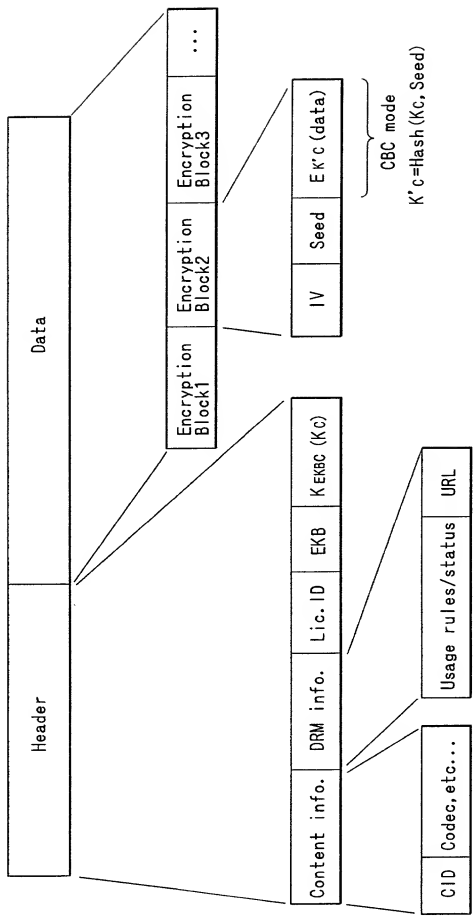


FIG. 6

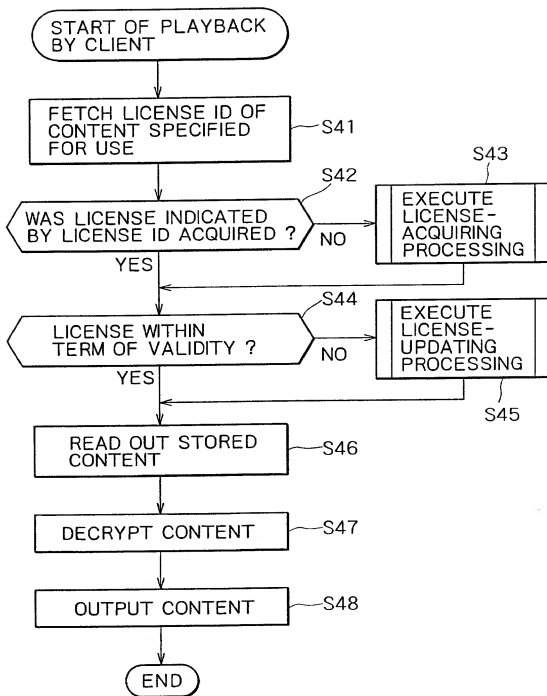


FIG. 7

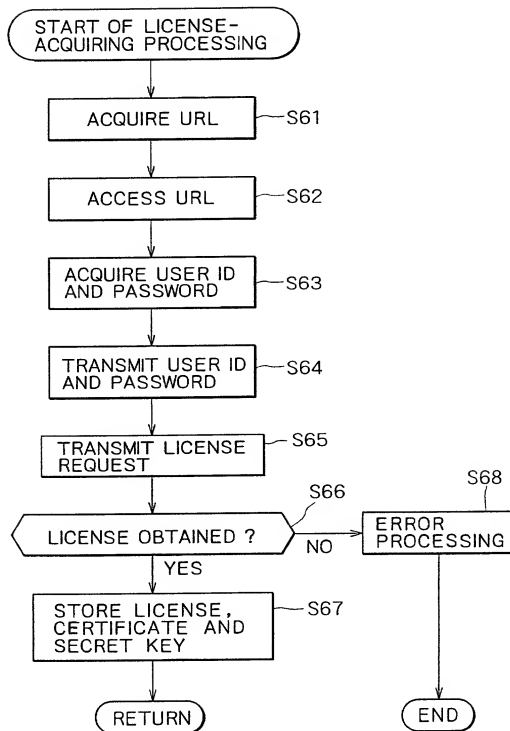


FIG. 8

LICENSE ID
CREATION DATE AND TIME
VALIDITY TERM
USAGE CONDITION
LEAF ID
DIGITAL SIGNATURE

FIG. 9

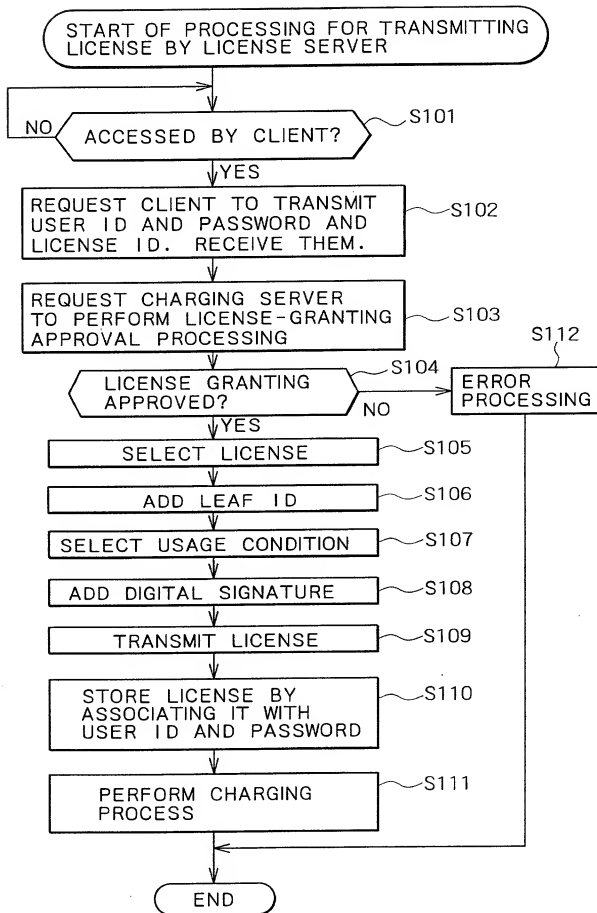
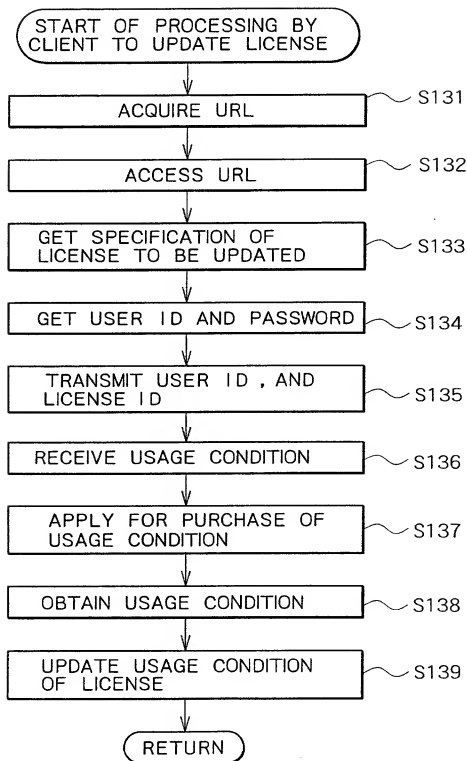


FIG. 10



10072105.020602

FIG. 11

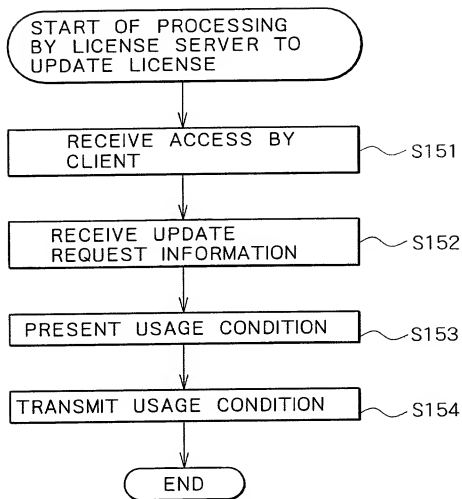


FIG. 12

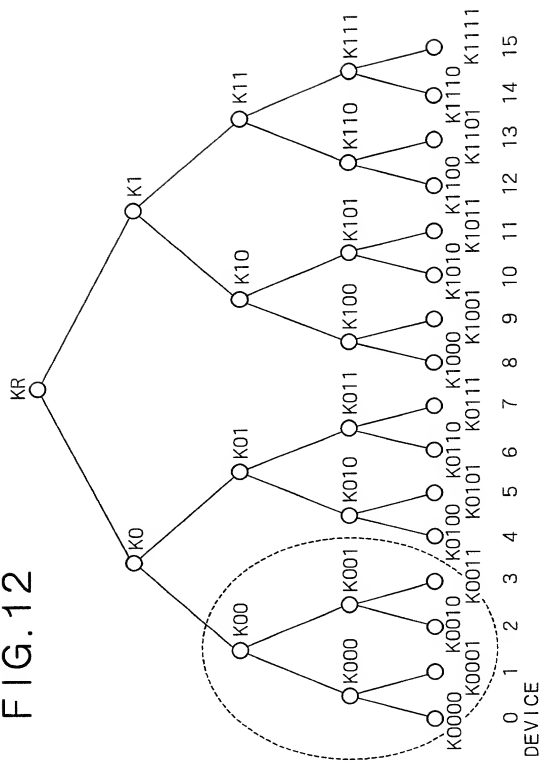


FIG. 13

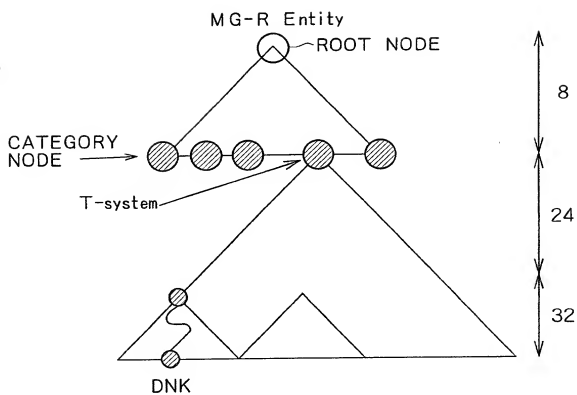


FIG. 14

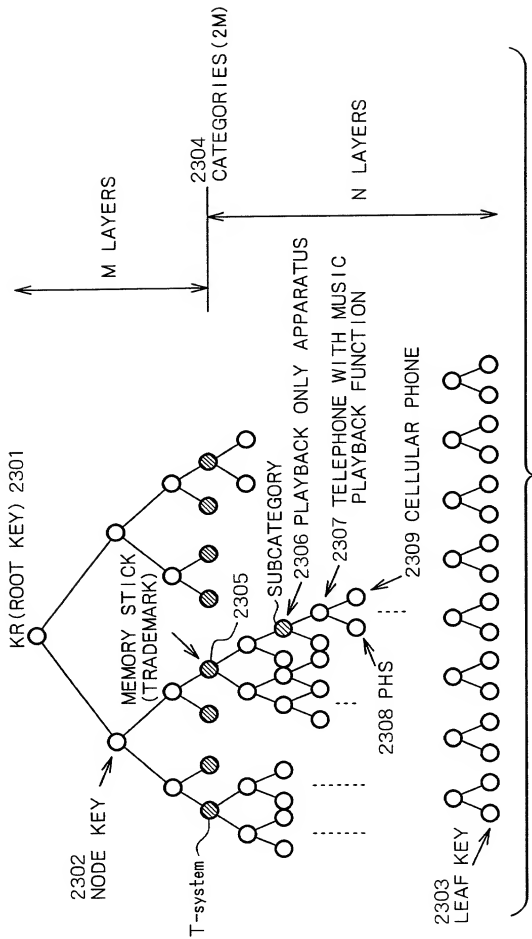


FIG. 15A

EKB (ENABLING KEY BLOCK)
TRANSMISSION OF NODE KEYS OF VERSION
t TO DEVICES 0, 1 AND 2

VERSION:t	
INDEX	ENCRYPTION KEY
0	$E_{nc}(K(t)0, K(t)R)$
00	$E_{nc}(K(t)00, K(t)0)$
000	$E_{nc}(K000, K(t)00)$
001	$E_{nc}(K(t)001, K(t)00)$
0010	$E_{nc}(K0010, K(t)001)$

FIG. 15B

EKB (ENABLING KEY BLOCK)
TRANSMIT NODE KEYS OF VERSION
t TO DEVICES 0, 1 AND 2

VERSION:t	
INDEX	ENCRYPTION KEY
000	$E_{nc}(K000, K(t)00)$
001	$E_{nc}(K(t)001, K(t)00)$
0010	$E_{nc}(K0010, K(t)001)$

FIG. 16

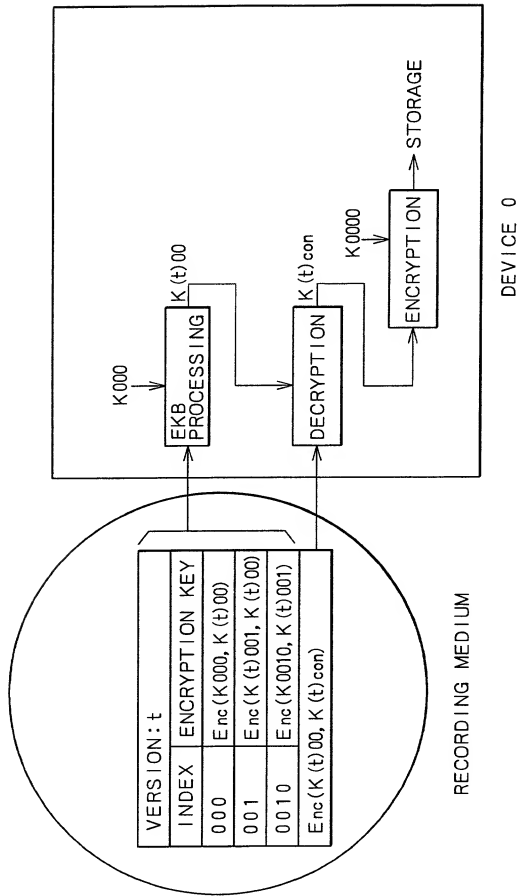
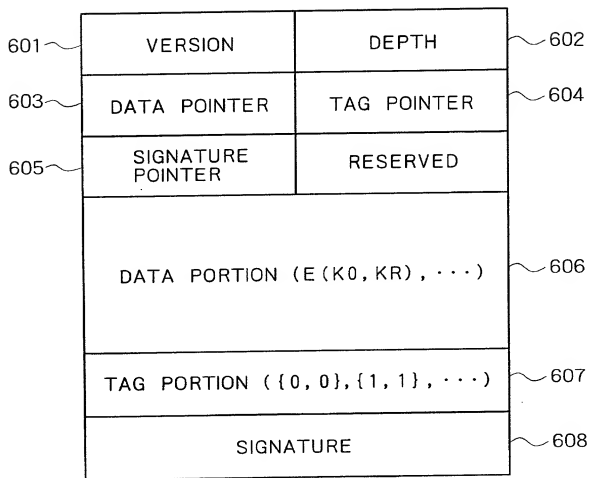


FIG. 17



EKB

10072409-020802

FIG. 18A

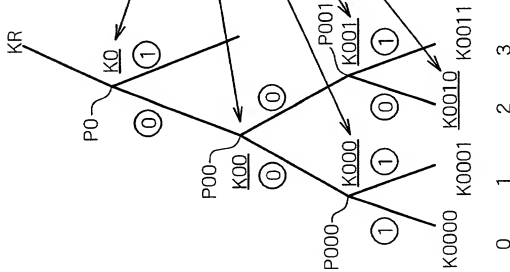


FIG. 18B

EKB (ENABLING KEY BLOCK)

TRANSMISSION OF NODE KEYS
OF VERSION t TO DEVICES 0,
1 AND 2

TOP NODE ADDRESS: KR	
DATA (ENCRYPTION KEY)	TAG
$Enc(K(t)0, K(t)R)$	{0, 1}
$Enc(K(t)00, K(t)0)$	{0, 0}
$Enc(K(t)000, K(t)00)$	{1, 1}
$Enc(K(t)0001, K(t)00)$	{0, 1}
$Enc(K(t)0010, K(t)001)$	{1, 1}

↓

{L TAG, R TAG}
L TAG AND R TAG ARE
EACH 0 TO INDICATE
EXISTENCE OF DATA OR
1 OTHERWISE

FIG. 18C

DATA: $Enc(K(t)0, K(t)R)$, $Enc(K(t)00, K(t)0)$, ...
TAG: {0, 1}, {0, 0}, {1, 1} ...

FIG. 19

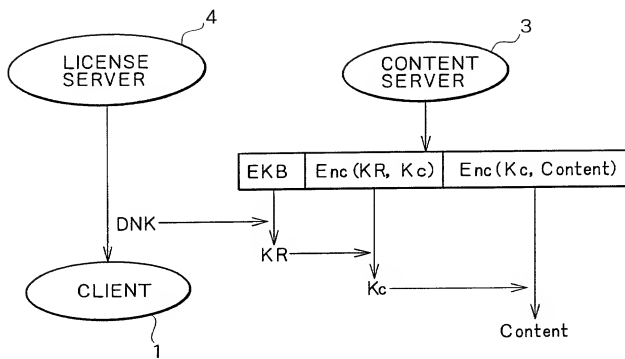


FIG. 20

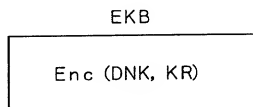


FIG. 21

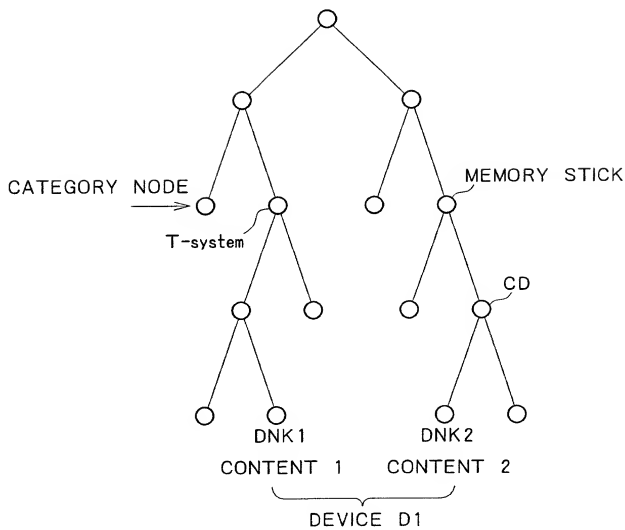


FIG. 22

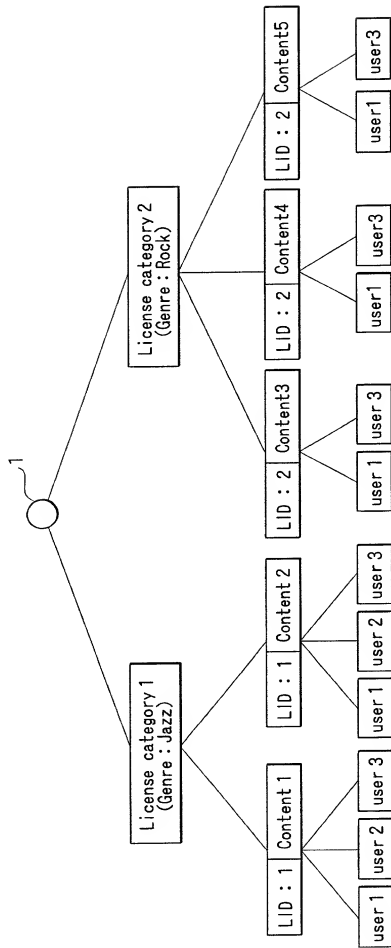


FIG. 23

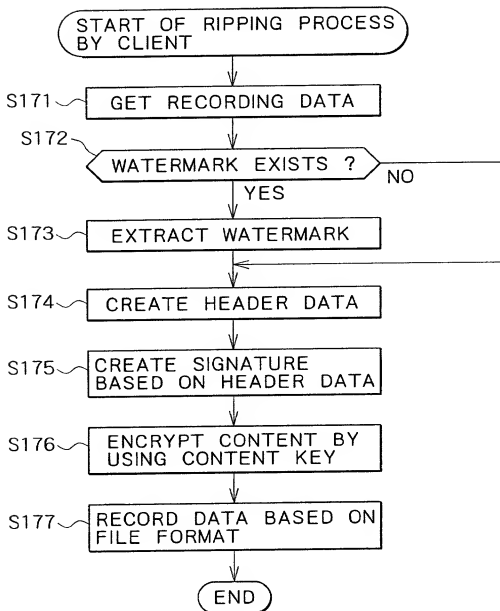


FIG. 24

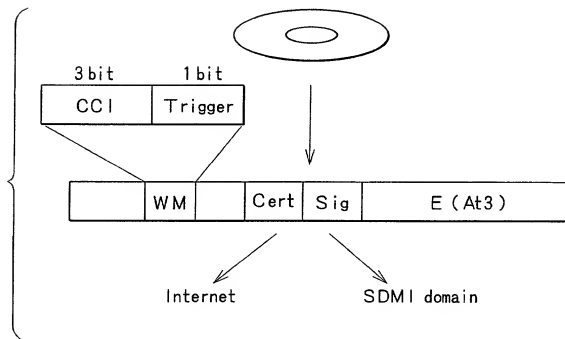


FIG. 25

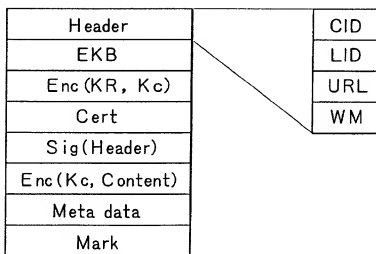


FIG. 26

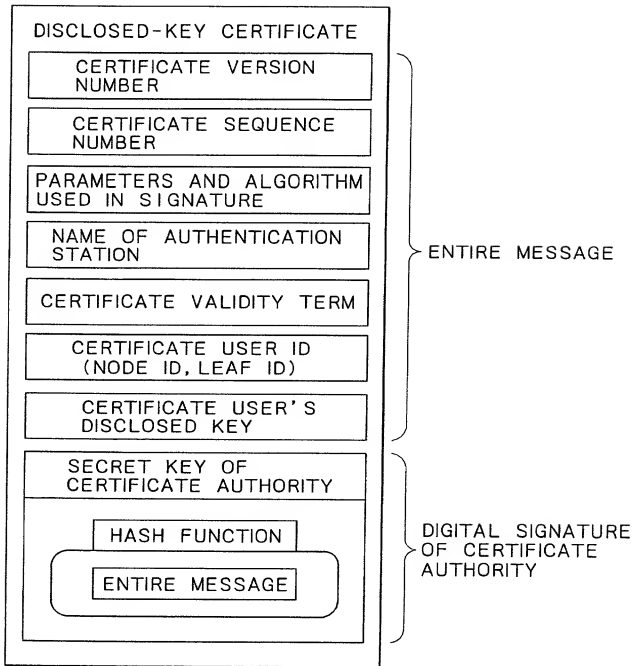


FIG. 27

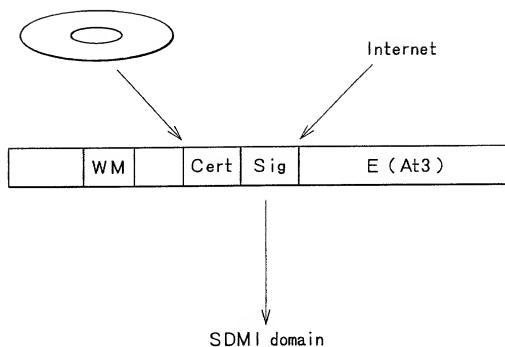
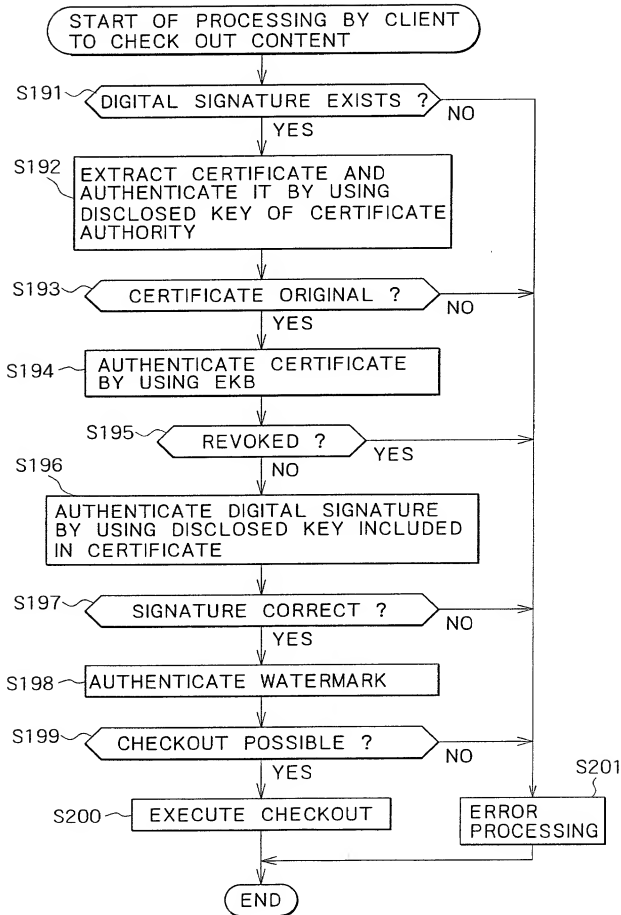


FIG. 28



2007-2-19 10:20:02

FIG. 29

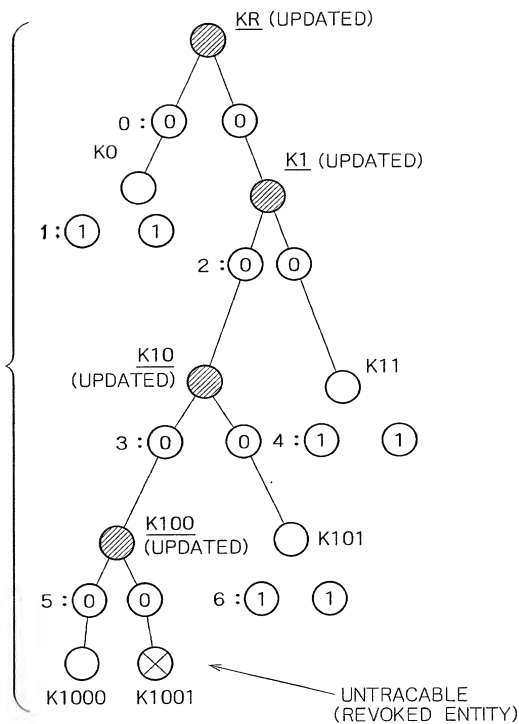


FIG. 30

DATA PORTION AND TAGS OF EKB
(ENABLING KEY BLOCK)

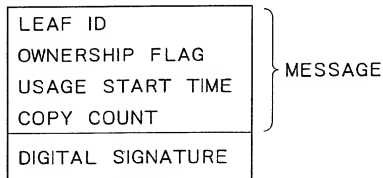
DATA (ENCRYPTED KEYS)	$\text{Enc}(K0, K(t)R, \text{Enc}(K(t)1, K(t)R))$ $\text{Enc}(K(t)10, K(t)1), \text{Enc}(K11, K(t)1)$ $\text{Enc}(K(t)100, K(t)10), \text{Enc}(K101, K(t)10)$ $\text{Enc}(K1000, K(t)100)$
TAGS	$0 : \{0, 0\}, 1 : \{1, 1\}, 2 : \{0, 0\}, 3 : \{0, 0\}$ $4 : \{1, 1\}, 5 : \{0, 1\}, 6 : \{1, 1\}$



{ L TAG, R TAG }

L TAG AND R TAG ARE EACH 0 TO INDICATE
EXISTENCE OF DATA OR 1 OTHERWISE

FIG. 31



MARK

FIG. 32

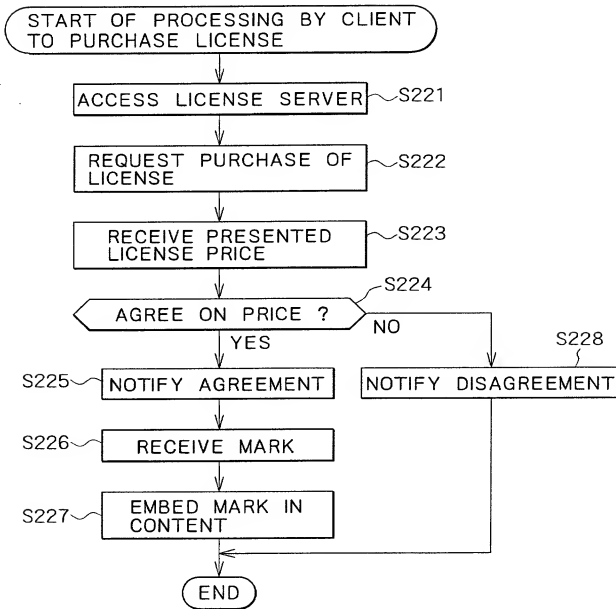
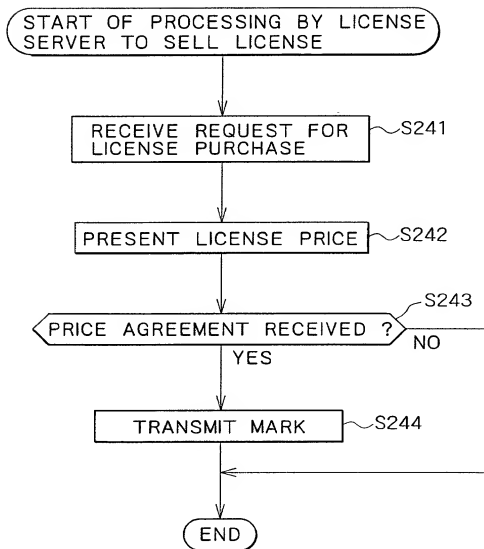


FIG. 33



10072409 020802

FIG. 34

Mark = {LeafID, Own, Sig_s(LeafID, Own)}

FIG. 35

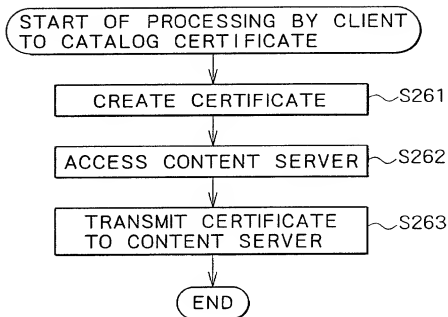


FIG. 36

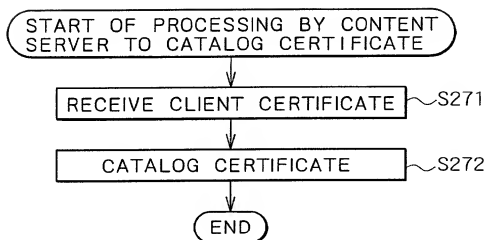


FIG. 37

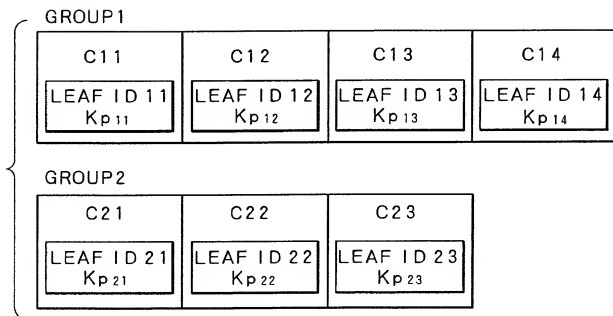


FIG. 38

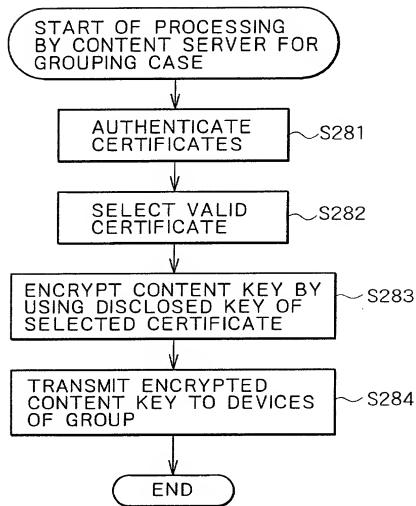


FIG. 39

$Enc(K_{p11}, K_c), Enc(K_{p12}, K_c), Enc(K_{p13}, K_c)$

FIG. 40

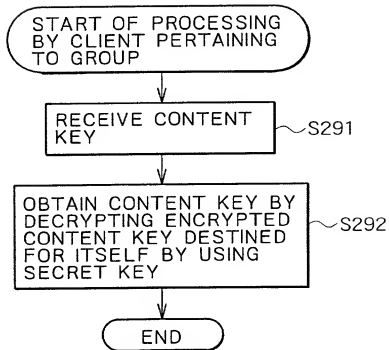
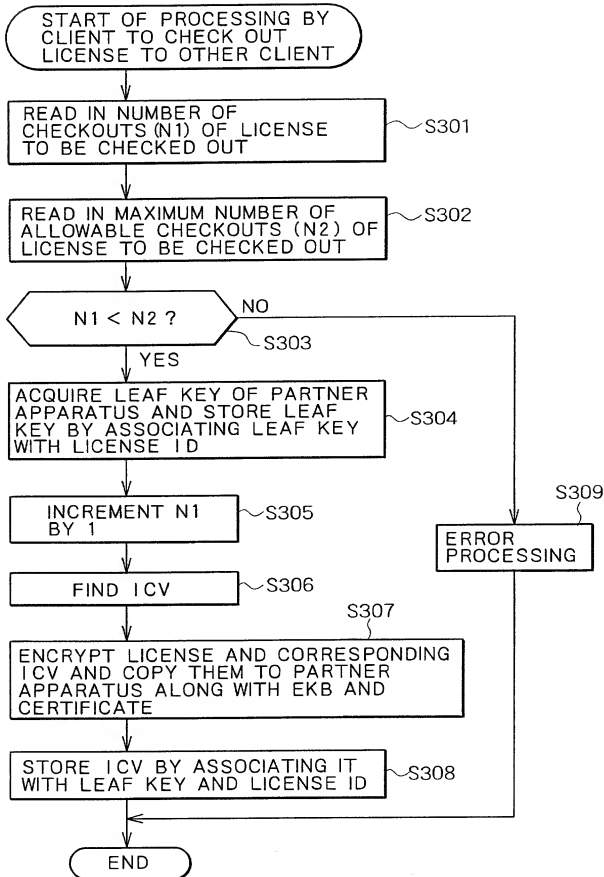


FIG. 41



10072409 020802

FIG. 42

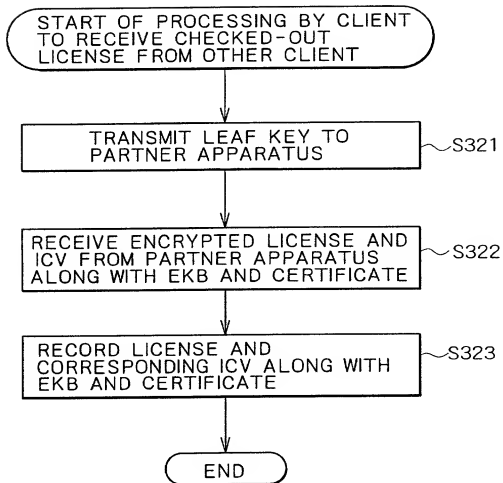


FIG. 43

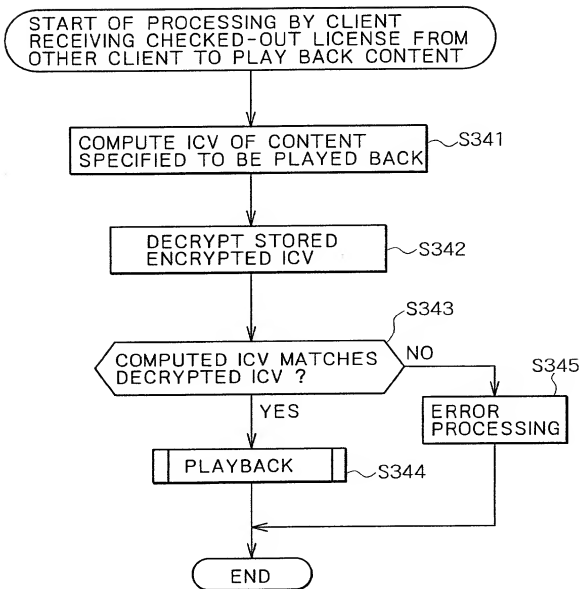


FIG. 44

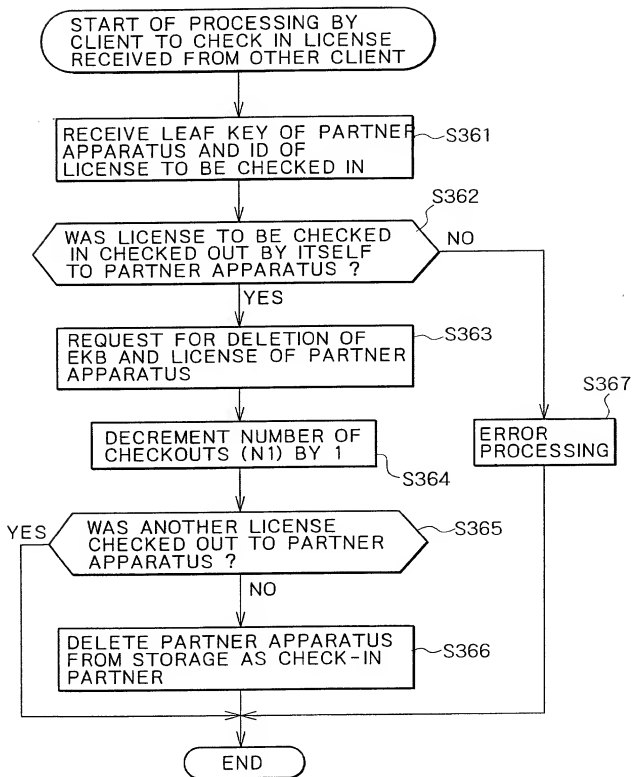


FIG. 45

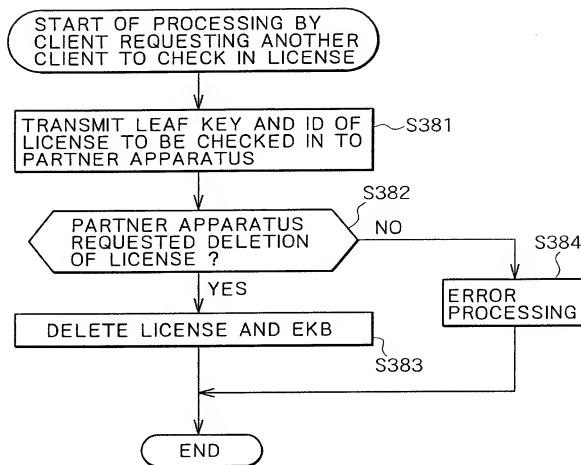


FIG. 46

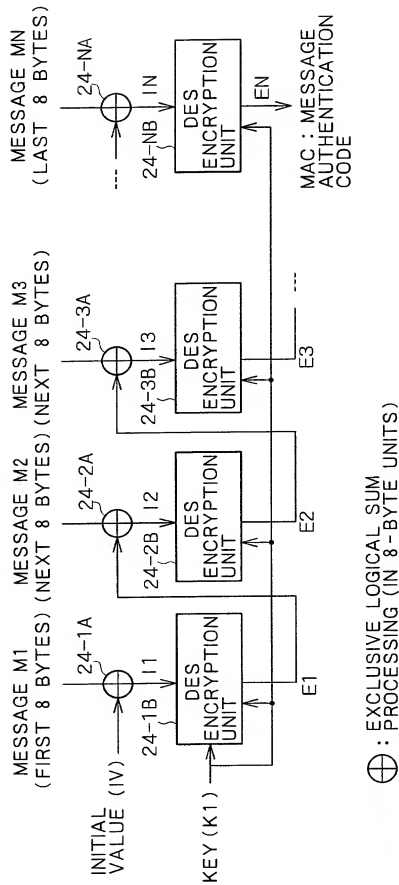


FIG. 47

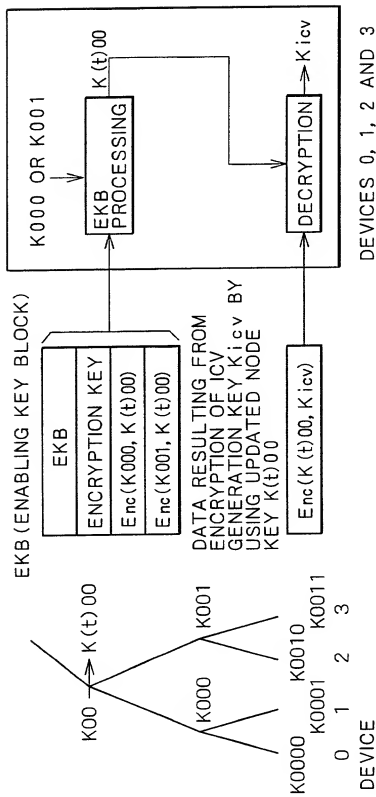


FIG. 48

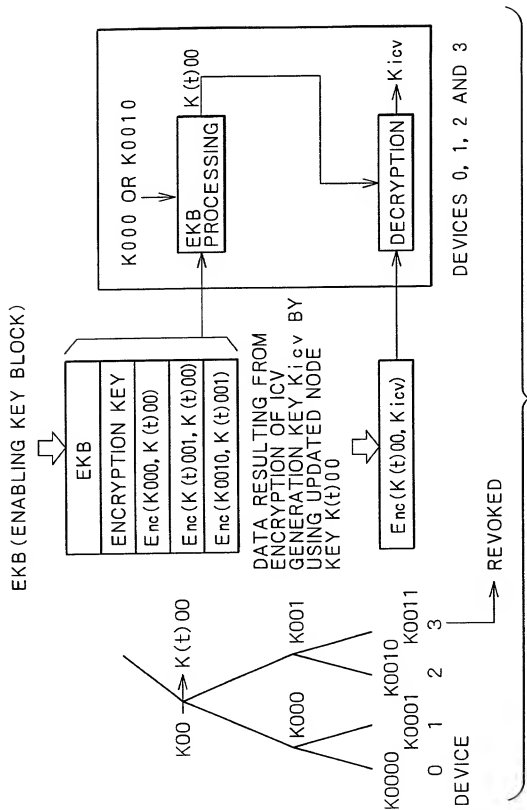


FIG. 49A

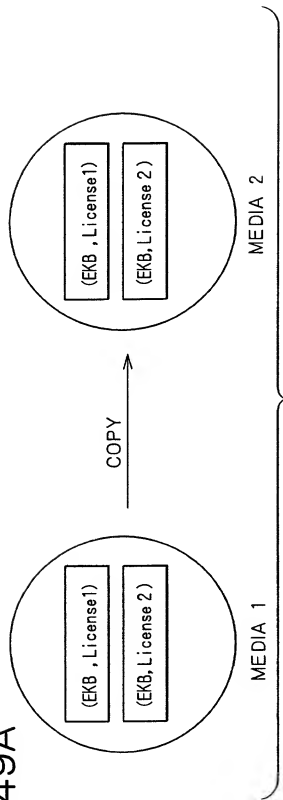


FIG. 49B

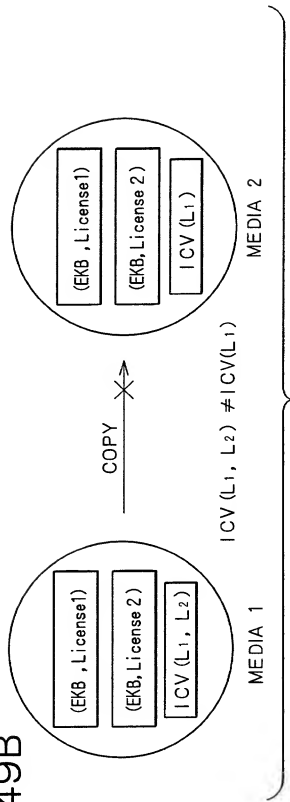


FIG. 50

